

BEST AVAILABLE COPY

RECEIVED

NOV 1 9 2001

Technology Center 2100

GAU 2131

ATTORNEY DOCKET NO .:

06944.0038

IN THE UNITED STATES PATENT & TRADEMARK OFFICE

In re patent application of:

Robert Lambert et al.

Serial No.:

09/900,959

Group Art Unit:

2131

Filed:

July 10, 2001

Examiner:

Unknown

Title:

METHOD AND APPARATUS FOR MINIMIZING

DIFFERENTIAL POWER ATTACKS ON PROCESSORS

Commissioner of Patents and Trademarks Washington, D.C. 20231

Dear Sir:

INFORMATION DISCLOSURE STATEMENT

Pursuant to the duty to disclose under 37 CFR §1.56, Applicant submits herewith a Form PTO/SB/08A listing references of which the Applicant is aware and which are brought to the attention of the Examiner. In accordance with 37 CFR §1.98(a)(2), a copy of each document listed in the enclosed Form PTO/SB/08A is submitted herewith.

Pursuant to 35 USC §120, this application relies on the earlier filing date(s) of the following prior application(s):

Serial Number

Filing Date

· PCT/CA00/00021

1/11/00

·PCT/CA00/00030

1/14/00

The filing of this IDS shall not be construed as a representation that a search has been made, an admission that the information cited is, or is considered to be, material for patentability, or that no other material information exists. This filing shall not be construed as an admission against interest in any matter.

BEST AVAILABLE COPY

2

This IDS is submitted pursuant to 37 CFR §1.97(b) and, accordingly, no fee is believed to be due for consideration of the documents submitted herewith.

Applicant respectfully requests consideration of the items listed and requests the Examiner to return a copy of the attached Form PTO/SB/08A after being marked as being considered by the Examiner.

Respectfully submitted,

Date: October 16, 200 /

Registration No. 20,33% Agent/Attorney for Applicant

type a plus sign (+) inside this box	+	Ţ.	7				
--------------------------------------	---	----	---	--	--	--	--

type a plus sign (+) inside this box

Approved :e through 10/31/2002. OMB 0851-0031

Patent and Trademark Cinica: U.S. DEPARTMENT OF COMMERCE

Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449A/PTO

INFORMATION DISCLOSURE (use as many sheets as non----

Complete if Known			
Application Number	09/900,959		
Filing Date	July 10, 2001		
First Named Inventor	LAMBERT, Robert		
Group Art Unit	Not Yet Assigned		
Examiner Name	Not Yet Assigned		
Attorney Docket Number	06944.038		

NT &	U.S. PATENT DOCUMENTS					
Examiner Initials		l Number .	ument d Code ² known)	Name of Patentee or Applicant of Cited Document	Date of Publication of Cited Document MM-DD-YYYY	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		5 675 645	A	Schwartz et al.	10-07-1997	
		4 519 036	Α	Green, Ian M.	05-21-1985	
		5 202 995	A	O'Brien, John K.P.	04-13-1993	RECEIVED
		5 511 198	Α	Hotta, Kohlchiro	04-23-1996	
		5 524 222	A	Hervin	06-04-96	NOV 1 9 2001
		5,650,948		Gafter	07-22-97	
			-			Technology Center 2100
			-			
					 	
			+		-	
						:
			+			
 			┼╌┤		 	
				·		

i				FOR	EIGN PATENT DOCUMEN	TS		
	-		Foreign Patent Document Name of Patentee or Date of				Pages, Columns, Lines, Where Relevant	П
Examiner Initials	Cite No.1	Office	Kind Code ^a Number ⁴ (# known)		Kind Code Applicant of Cited Document Cited Document		Passages or Relevant Figures Appear	Τ ⁶
		wo	98 52319	Α	Fleit, Lois	11-19-1998		
	•	FR	2 672 402	A	Gemplus Cord INT	08-07-1992		
	٠,٠	wo	98 00771	Α	Northern Telecom Ltd/	01-08-1998		
					· · · · · · · · · · · · · · · · · · ·			$oldsymbol{oldsymbol{oldsymbol{eta}}}$
							 	↓
						 		┿
						 		+
 								+-
 			<u> </u>					+
						<u> </u>		1

Examiner	Date	
Signature	Considered	

Burden Hour Statement: This form is estimated to take 2.0 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U. S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.

^{*}EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ Unique citation designation number. See attached Kinds of U.S. Patent Documents. ³ Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). 4 For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. 5 Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. ⁶ Applicant is to place a check mark here if English language Translation is attached.

PTO/SB/08B (08-00) use through 10/31/2002. CMB 0651-0031 uce: U.S. DEPARTMENT OF COMMERCE

Approv. Jise through 10/31/2002. CMB 0651-0031

Patent and Trademan Line: U.S. DEPARTMENT OF COMMERCE

Juder the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid CMB control number.

Substitute for form 1449B/F I O

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

Complete If Known			
Application Number	09/900,959		
Filing Date	July 10, 2001		
First Named Inventor	LAMBERT, Robert		
Group Art Unit	Not Yet Assigned		
Examiner Name	Not Yet Assigned		
Attorney Docket Number	06944.038		

<u>*/</u>	OTHER PRIOR ART NON PATENT LITERATURE DOCUMENTS				
Examiner Initials*	Cite No.1	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	Τ²		
		PAUL KOCHER, JOSHUA JAFFE, and BENJAMIN JUN, Introduction to Differential Power Analysis and Related Attacks, http://www.cryptography.com/dpa/technical/index.html, 1998, San Francisco.			
· · ·	,	PAUL KOCHER, Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and other systems, http://www.cryptography.com//timing attack/paper.html, Downloaded November 11, 1998, San Francisco.			
		JOHN WHARTON, An introduction to the IntelR MCS-s1TM Single-Chip Microcomputer Family, Intel Application Note AP-69, may 1980, USA.			
**		RECEIVED	t		
· · · · · · · · · · · · · · · · · · ·		NOV 1 9 2001	L		
		Technology Center 2100			
			ľ		
·····		-			

Examiner	 Date	
Signature	Considered	

Burden Hour Statement: This form is estimated to take 2.0 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U. S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.

BEST AVAILABLE COPY

^{*}EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ Unique citation designation number. ² Applicant is to place a check mark here if English language Translation is attached.